jamk.fi

Improvement of Information Security Management System in Media X Corporation

Author: Harri Henttinen

Master's Thesis
April 2018
Technology, Communication and Transport
Degree Programme in Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Henttinen, Harri	Master's thesis	April 2018
		Language of publication: English
	Number of pages: 50	Permission for web publication: Yes

Title of publication

Improvement of Information Security Management System in Media X Corporation

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Hautamäki, Jari

Assigned by

Hännikäinen, Anne

Abstract

This Master`s thesis was carried out as a result of Media X Corporation (anonymized) ISMS, Information Security Management System improvement project. The topic of the thesis was accepted in JAMK, University of Applied Sciences in September 2017. Some of the material of this document has been declared as company confidential by original assignor and is not available in this document.

The purpose of this thesis was to provide a current state analysis for the existing Media X Corporation Information Security Management System and to give guidance for the existing model improvement work.

In the beginning of this thesis, the business areas of Media X Corporation and their organization as well as their technical functions are explained. In the theory part of this thesis several popular and world-wide Security Frameworks are introduced and compared and their main characteristics and suitability for Media X Corporation purpose is evaluated as well as discussed shortly the pros and cons of the Frameworks to be utilised as a basis of ISMS. ISO/IEC 27001 standard was found as the most suitable framework for Media X.

In the practical current state analysis work the ISO 27001 standard and ISO 27002 best practices were used as main criteria for the evaluation and assessment of the exiting ISMS. The evaluation results revealed several security controls area gaps and results are presented in current state analysis report, which was provided to Media X Corporation.

Keywords/tags

Cybersecurity, Information Security, Network Security, Information Assurance, ISO 27000, ISO 27001, ISO 27002, Current State Analysis, Security Framework.

Miscellaneous. The following appendices and tables have been declared as confidential by Media X Corporation and have removed from the public part of this Master's Thesis document: Appendix 5, Appendix 6, Appendix 7, Appendix 8, Appendix 9, Table 2, Table 4, Table 6, Table 7, Table 8, Table 9, Table 10, Table 11, Table 12, Table 13, Table 14

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Henttinen, Harri	Opinnäytetyö, ylempi AMK	Huhtikuu 2018
	Sivumäärä 50	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Information Security Management System Improvement in Media X Corporation

Tutkinto-ohjelma

Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Hautamäki, Jari

Toimeksiantaja(t)

Hännikäinen, Anne

Tiivistelmä

Tämä opinnäytetyö tehtiin Media X Oy:lle (nimi muutettu) tehdyn tietoturvan hallintajärjestelmän parannus -projektin perusteella.

Tavoitteena oli suorittaa nykytila-analyysi Media X Oy:n nykyiselle tietoturvan hallintajärjestelmälle sekä löydösten ja havaintojen perusteella tehdä parannusehdotuksia nykyisiin tietoturvajärjestelyihin.

Opinnäytetyössä on esitelty lyhyesti Media X Oy:n toiminnot ja arvioitu erilaisten tietoturvan viitekehysten soveltuvuutta nykytilan arviointiin.

Soveltuvimmaksi todettiin ISO 27001-standardin mukainen järjestely. Nykytila-analyysi tehtiin kyseisen ISO-standardin määritysten mukaisesti ja organisaatiossa havaittiin puutteita eri alueiden tietoturvakyvykkyyksissä. Analyysin tuloksena dokumentaatioon, prosesseihin, IT-omaisuuden hallintaan, henkilöstön tietoturvallisuusosaamiseen ja -tietoisuuteen sekä tietoturvallisuusriskienhallintaan ehdotettiin parannuksia.

Nykytila-analyysin tulokset toimitettiin Media X Oy:lle erillisellä raportilla. Varsinainen nykytila-analyysiraportti on julistettu luottamukselliseksi Media X Oy:n toimesta ja ei näin ollen ole mukana opinnäytetyön julkisessa versiossa.

Opinnäytetyön lopussa on arvioitu projektia kokonaisuutena sekä nykytila-analyysin havaintoja ja löydöksiä yleisemmin sekä parannusehdotuksia Media X Oy:n kannalta.

Avainsanat (asiasanat)

Nykytila-analyysi, ISO/IEC 27001, ISO/IEC 27002, tietoturvaviitekehys, tietoturva, kyberturvallisuus, verkkoturvallisuus.

Acronyms

B2B	Business to Business
B2C	Business to Consumer
CISO	Chief Information Security Officer
DTI	Department of Trade and Industry
EU	European Union
FIPS	Federal Information Processing Standard's
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
IEC	International Electro Technical Commission
ISO	International Organization for Standardization
IT	Information Technology
PDCA	The Plan-Do-Check-Act
SAQ	Self-Assessment Questionnaire
SBS	Media X Business Solutions
SFS	Suomen Standardisoimisliitto SFS ry
SMN	Media X Media Netherlands
SOA	Statement Of Applicability
SOX	Sarbanes-Oxley
QSA	Qualified Security Assessor

Contents

Figures

Tables

1 Introduction

This Master's thesis work related current state evaluation project was done as assignment of Media X Corporation Chief Information Security Officer (CISO) and it was accomplished between November 2016 and April 2017. The Master Thesis work supervisor in Media X Corporation side was acting Senior Security Manager, Media X Corporation Infrastructure Security.

The thesis describes Media X's improvement project of Corporation Information Security Management System (ISMS) related the phases and results of the current state of the evaluation project. The findings of the security assessment performed for the Media X Corporation as part of the ISMS improvement activities. The current state security assessment has been done by Harri Henttinen (M.Sc.) and the results are reported in *Information Security Management System Current State report* document dated 30 of March 2017.

The report content is classified as *Confidential* by Media X Corporation and hence, it is not included to this Master Thesis work as such, albeit the generic findings are presented in *Analysis Results* and *Conclusions* section of this Master Thesis, but the report itself containing the detailed findings and related recommendations that were obtained in accordance with the project scope and approach are not included in here. The same apply also for the Current State Analysis tool defined for this particular project. Also, appendices from 5 to 9 as well the tables 2, 4 and from 6 to 14 referred in this document are classified as *confidential* by original assigner and are not available in this Master Thesis document for confidentiality reasons.

Information Security Management System is a standardized, risk-based security governance and development program, executed within a corporate governance and operative level organization and functions. Standard starting point for the program is to define company assets and threats against those assets to find out the risk level and further on identify relevant information security controls to reduce the risks to accepted level. The basic assumption is that ISMS is a continuous improvement process after the ISMS establishment phase.

Before starting any risk assessment, it is important to have visibility enough to the existing information security control situation. By information security controls is meant all information security related processes, control devices, procedures, tools, security awareness and governance of security organization. To get the missing knowledge about the above-mentioned visibility, the *Current State Analysis* need to be done for the information security area.

The Current State analysis study described in this Thesis Work is done by interviewing Media X Corporation key persons in different IT, security and governance organization and recording the findings to the specific tool. In addition, the Media X Corporation information security related documentation was reviewed and analysed.

The information security interview questions are based on the controls defined in ISO 27002 standard of best practices document. The Current State analysis related evaluation tool is developed particularly for this project to better fit for the purpose within Media X Corporation business organization.

The Current State of Media X Corporation information security described in this Master Thesis is reflecting the situation in fall 2016 and many security control area improvements have executed since then until the date writing this thesis during the spring 2018.

2 Media X Corporation

Media X Corporation is a consumer media and learning solution company in Finland, but it has business activities also outside Finland in the other parts of Europe. There are two main business areas, *Media* and *Learning*. In Finland and in the Netherlands Media X is market leading media company with several different media platforms starting from TV and Web based media to different kind of press media, such as newspapers and magazines. Media X learning area main markets are in Belgium, Finland, the Netherlands, Poland and Sweden. Millions of consumers and customers use Media X entertainment, information and education solutions and services daily. Media X Corporation is employing over 5, 000 persons at the moment (Media X 2017).

Figure 1. presents Media X Corporation main business units and technical functions within them, which are focused with more detailed within this study.

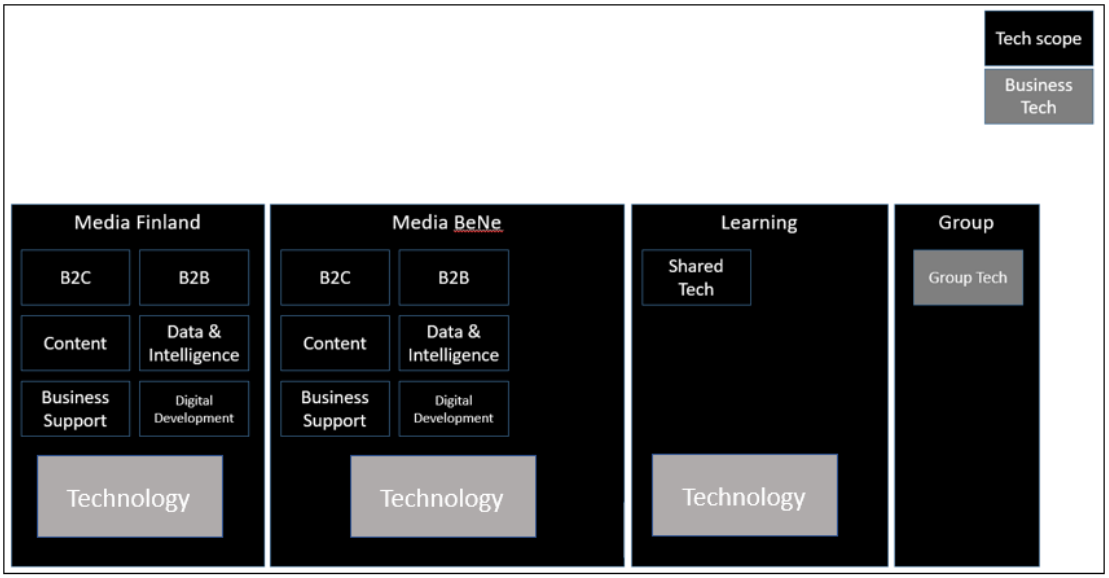


Figure 1. Media X Corporation business units and technical functions (Media X Corporation)

Media X Organization and Functions

Media X consists of two segments, *Consumer Media* and *Learning*, and three Strategic Business Units: *Media X Media BeNe*, *Media X Media Finland* and *Media X Learning* (Media X).

There are also included non-core operations, such as real estate companies, head office functions and group eliminations. Media X Corporation is the Parent Company of the Media X Group. In the scope of this study the Media X Media Finland and Media X Media BeNe as Media X Corporation parts are included.

Media X Media is offering wide variety of media, newspaper publishing, magazine publishing, printing, TV and radio, online gaming and other apps, digital services and other online operations. Media X Media was formed by the merger of former Media X Magazines, Media X News and Media X Entertainment divisions.

Media X Learning Business Unit is concentrating an educational publishing, publishing and business information and services markets. Media X Learning products and

solution provide different kind of learning solutions that are developed especially co-operation with pupils and teachers.

Media X's consolidated balance sheet total was 2,605.6 million €'s at the end of the year 2016 versus net sales was € 1639.1 million in the same year (Media X 2017).

Generic Media X Security Situation

At the time, the current state analysis was done, there was no formal corporate-wide ISMS available, but several information security controls and best practices implemented separately within several different Media X Corporation business domains and teams.

There were security practises and technical controls in place but organizational issues affect the overall security situation and responsibilities were not defined clearly enough. In many cases, appropriate security practises were identified but not consistently implemented, documented and continuously practised. The main root cause for this was lack of coherent security risk assessment procedures. Risk assessments had been carried out for some components, mainly for the financial systems, but it was not a continuous process at that moment. As observation, the risk assessment scope should cover also business impacts of information security risks.

In Media X Corporation there are some security controls outsourced to third party. For these controls there were no sufficient visibility. In some specific areas, controls and practices were in better condition, but from ISMS perspective as a whole not.

3 Objective of the Study

The objective of this ISMS improvement assignment was to review the security posture of Media X Corporation ISMS from ISO 27001 standard point of view. As an assessment framework, two baselines were applied: ISO 27001 standards and ISO 27002 code of practices.

The Media X Corporation main development targets and the main targets for the study were set up as follows:

- To accomplish a current state analysis of the existing Information Security arrangement within Media X Corporation
- To define possible gap between real security control situation and standard requirements
- According to the gap analysis work to suggest some improvement for the existing Information Security arrangement
- Add visibility about the existing Information Security arrangement to guide the Media X organization towards the ISO 27001 ISMS standard alignment
- To rise security awareness within Media X Corporation by running the current state analysis interviews.

4 Research Method Used in the Study

There are different kind of research methods available, such as *Historical, Comparative, Descriptive, Correlation, Experimental, Evaluation and Action methods.* Part of them are quantitative methods, such as *Correlation* and *Experimental* whereas others are qualitative ones (Clarke 2005).

In this study *Evaluation* has been chosen as a research method. It is a quantitative method, that is mostly used for gathering of information, surveys, interviews and questionnaires. In this method, the evaluation tool is used as a measuring instrument and results are recorded to test against existing theories; in this study against the ISO 27001 and ISO 27002 recommendations. Finally, the relevant conclusions are drawn from the results (Faculty of Commerce, 2012).

Evaluation is a research method that fits for this kind of comparative study, where the target data of the study is a combination of processes, human competences, physical tools, interview results and related documentation.

There are two types of *Evaluation* methods, *System Analysis* and *Responsive Evaluation. System Analysis* is a holistic type of research, which is realized in a three-stage order and is typical for scientific enquiry, which in practice means breaking the

problem question into more researchable parts, which are then evaluated separately. In the next phase the parts of evaluations are aggregated into one explanation of the whole. The system analysis is involved with (Clarke 2005):

- Identifying the encompassing the whole (system) of which the phenomenon or problem is a part.
- Evaluating the behaviour or properties of the encompassing whole.
- Explaining the behaviour of properties of the phenomena or problem in terms of its roles or functions within the encompassing whole.

The other *Evaluation* method is called *Responsive Evaluation.* In that method, series of investigative steps are undertaken in order to evaluate, how responsive a target is to all defined requirements taking part in it (Clarke 2005):

- Data collection: Identifying issues from the people directly involved in the activity or program; identifying further issues from process or program documents; observing how the activity or programme is actually working.
- Evaluation: The design and content of an evaluation based on the data collected and reporting findings, e.g. the form or format of the report.
- Suggested changes: Informing the participants of the findings in ways specifically designed for each type of audience, e.g. top management of the company.

The *Responsive Evaluation* method fits for the assessment of the organization of Media X Corporation to meet the standard requirements best and provides the solution proposal of the problems to be solved, hence, it is the used research method for this current state study.

5 Security Frameworks

An information security framework is a set of documented, agreed and understood policies, procedures, and processes defining the ways information is managed within a business organization. The main target is to lower the risk and number of vulnerabilities and increase confidence throughout the organization. There are about 250 different security frameworks developed and used globally to suit a wide variety of businesses and sectors (Originit 2017).

Definition of Security Framework

The National Institute of Standards and Technology, NIST has defined the Security Framework as a risk-based approach to reduce cybersecurity risks. It is composed of following parts: The *Framework Core*, *the Framework Profile*, and the *Framework Implementation Tiers*. Sometimes it is also called as the “Cybersecurity Framework.”

The Security Framework consists of different cybersecurity activities and desired outcomes as well as commonly applicable references within critical infrastructure sectors. (NIST 2017, 3-5).

Framework Core is the Framework Core consists of four different element types: Functions, Categories, Subcategories, and Informative References. The Core presents industry standards, guidelines, and practices allowing communication across the organization from the executive level to the operative implementation level.

When considered together, the above-mentioned elements provide a strategic, high-level view to the organization's cybersecurity risk management lifecycle (NIST 2017, 3-5).

Framework Profile is the representation of the outcomes from Framework Categories and Subcategories that a particular system or organization has selected. It can be characterized as the alignment of standards, guidelines, and practices in a particular implementation scenario. The existing organization security posture can be improved by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). By developing a Profile, an organization can review all Categories and

Subcategories and, based on a risk assessment and information on business drivers, determine the most important ones for the organization.

Categories and Subcategories can also be added to better address the organization risks as well as support the prioritization and measurement of progress toward the Target Profile. Profiles can be used as self-assessments and communication within and outside the organization. The Current Profile can be used to support the planning of other business criteria, such as cost-effectiveness and innovation (NIST 2017,3-5).

Framework Implementation Tier is the approach the organization has taken to identify and manage the risks. Tiers describe an organization's cybersecurity risk management practices defined in the Framework exhibiting the characteristics, e.g. risk and threat aware, repeatable, and adaptive. Within the Tier selection process, an organization´s current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints should be considered. The Framework Implementation Tiers are not intended to be maturity levels, but they are supposed to provide guidance in organizational interactions and coordination between cybersecurity risk management and operational risk management (NIST 2017, 3-5).

Comparison of Different Security Frameworks

There are several different security frameworks dealing with the problematics related to information security area. The most commonly used and major information security standards are ISO 27001, BS 7799, PCI DSS, ITIL and COBIT. In addition, the US based NIST SP 800-53 is very much referred security standard. Appendix 2. contains comparison table of the five most common ones.

Criteria to pick up some specific standard to be followed mostly depends on the business environment and possible field regulation requirements the organization is involved in. For example, some security frameworks are developed to health and care business, that needs to be compliant with HIPAA requirements whereas some other business needs to follow industrial standards, such as IEC 62443 for automation systems.

In addition, there are requirements such as PCI DSS for payment card industry standard, Sarbanes-Oxley (SOX) as well as many national administration level guidance and standards to be followed, such as German IT-Grundschutz standards, VAHTI and KATAKRI. New European Union (EU) General Data Protection Regulation is giving its own recommendations and demands in data protection and privacy area, which are supposed to be followed at a risk to get financial sanctions if not compliance with them.

From the information security point of view, different security frameworks cover mostly the needed security control areas; however, there are differences in the main focus they are concentrate on.

HITRUST, Health Information Trust Alliance has carried out a comparison from the perspective of health field (HiTrust 2017, 4). Even though carried out from health information point of view and gives an advance for HITRUST itself in the health standardization area, the other related results are general. HITRUST compared ISO/IEC 27001/2, NIST SP 800-53, and the HITRUST CSF frameworks.

The conclusions were that all frameworks are comprehensive and open frameworks, however, they differ substantially in some aspects, including *scope*, *industry specificity*, *level of integration and applicability*, *prescriptiveness*, *compliance*, *certification*, *shared assurance*, *assessment guidance*, *scaling*, *tailoring* and *tool support* (HiTrust 2017).

Table 1. describes the results of the comparison. The factor definitions of Table 1 are explained in Appendix 4.

Table 1. Comparison of HITRUST, ISO & NIST (HiTrust 2017)

Factor[1]	ISO/IEC 27001	NIST SP 800-53	HITRUST CSF
ISO 27001-Based	✓	✗	✓
Integrated Compliance Framework	✗	✗	✓
Healthcare Specific	✗[2]	✗[2]	✓[3]
Healthcare Standard	✗	✗[4]	✓
Prescriptive	✗[5]	✓	✓
Controlled Scaling	✗	✗	✓[6]
Controlled Tailoring	✗	✓[7]	✓
Control Compliance-Based	✗[8]	✓	✓
Organizational Certification	✗	✓	✓
Supports Third-Party Assurance	✓	✗	✓
Assessment Guidance	✗[9]	✓	✓
Tool Support	✗	✓	✓

Even though, HITRUST found CFS framework best for the health information field, they still trust ISO/IEC 27001 framework as a base for an information security management system (ISMS). This is because the ISO/IEC 27001 standard is an internationally accepted standard for the implementation and maintenance of ISMS and it provides high-level controls designed to suit almost any organization, in any industry, and in any country (HiTrust 2017).

Both NIST SP 800-53 and ISO/IEC 27001 provide information security standard requirement sets that are applicable to a wide scope of organizations and environments; however, NIST SP 800-53 controls are targeted specifically for U.S. government agencies (HiTrust 2017).

5.1.1 BS 7799

BS 7799 standard was originally published by British Standard Institution (BSI) Group in 1995. It was designed by the United Kingdom Government's Department of Trade and Industry (DTI). It consists of several parts. The first part contains the best practices for ISMS. It was revised in 1998 and eventually adopted by ISO as ISO 17799, "*Information Technology - Code of practice for information security management*." The second part of BS 7799, titled "*Information Security Management Systems* -

Specification with guidance for use" was published 1999. BS 7799-2 focused on implementing ISMS. It concentrates to the information security management structure and controls. The Plan-Do-Check-Act (PDCA) introduced in 2002 version of BS 7799-2 was also aligning it with ISO 9000 quality standard. Later in 2005 that standard became as ISO 27001 (Almunawar and Tuan, 2011).

5.1.2 COBIT5

COBIT, Control Objectives for Information and Related Technology is a high-level risk-oriented framework. Originally, it was used by IT governance professionals to help reduce technical risks. Later it became a standard to align IT business goals. COBIT maps core IT processes in a manner that allows governance bodies, such as business executives execute key policies and procedures. When ITIL and ISO 27002 are focusing only on information security, COBIT include IT management processes to the scope. COBIT is not as widely followed as other information security standards, yet, it is mostly used within the finance industry to comply with standards, such as Sarbanes-Oxley (SOX). It is useful when establishing business continuity plans (Origin 2017).

As for strengths for COBIT, it can be mentioned that COBIT is managed by ISACA (Information Systems Audit and Control Association) that keeps the standard up-to-date with technology development. It is a globally accepted standard and focuses on more than just the information security scope that other standards are limited to. Accordingly, COBIT can be easily implemented also partially without requiring a full analysis and commitment by the organization.

COBIT´s weakness is, that even though it is widely scoped it can also be a limiting factor during implementation. By design not limited to a single area, it can often lead to gaps in coverage. Generally, what it lacks is informative practical advice (Origin 2017).

5.1.3 ITIL

ITIL is a set of Information Technology Services Management (ITSM) concepts and best practices for IT development and IT operations. It consists of several books covering specific IT Service Management practices. One of those books focuses on best practices in Information Security.

ITIL follows a process-model to control and manage operations based on Plan-Do-Check-Act (PDCA) cycle credited by W. Edwards Deming. It contains eight main IT Services Management Standard and Best Practices components: Service Support, Service Delivery, ICT Infrastructure Management, Security Management, Application Management, Software Asset Management, Planning to Implement Service Management and Small-Scale Implementation (Almunawar and Tuan, 2011).

ITIL is offered in five core publications each dealing with different stage in the IT lifecycle. By ITIL process, one can generate documentation of processes, tasks and checklists, which are creating a baseline to implement controls and measure success. ITIL processes are generic and as such organization independent. (A Comparison of COBIT, ITIL, ISO 27002 and NIST, 2017).

The strength of ITIL is that it is the standard used worldwide and it may be considered for any company regardless of geographical location. It is created by U.K. government and therefore is a facile choice for the companies in the old British Commonwealth area of the world. ITIL´s most significant benefit is that it has increasing visibility into internal processes as well as management of them (A Comparison of COBIT, ITIL, ISO 27002 and NIST, 2017).

ITIL´s weakness is that it is a higher-level standard than ISO 27002, and in many process phases it refers to ISO standards for detailed implementation, thus lacking more detailed implementation recommendations and instructions.

5.1.4 ISO/IEC 27001

ISO 27001 standard is a framework focused on information security. It is developed by the International Standards Organisation (ISO). It is mature, very flexible, broad, solid, tried and tested and can be used across a several types and sizes of businesses, from companies under 100 employees through to around thousands of employees. The ISO 27001 specifies the ISMS requirements for documenting, establishing, implementing, operating, monitoring, reviewing, maintaining and improving it within an organization (Almunawar and Tuan, 2011).

The strength of ISO 27001 is that it is associated with a widely known standard of best practices ISO 27002, which was evolved from the British standard BS 7799 and defines

the necessary operational steps within an information security program. In addition, ISO 27001 is well recognized and understood by the other ISO/IEC standards users. ISO 27001 is easy to fit with the more widely known ISO 9000 quality standards for manufacturers introducing the security to quality process. By ISO 27001 standard it is possible to identify and mitigate gaps as well as possible overlapping issues in coverage (SearchSecurity 2017).

Weaknesses of ISO 27001 is its scope is limited specifically and purposefully to information security. For example, COBIT has a wider focus.

5.1.5 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard. It is defined by the Payment Card Industry Security Standards Council. It is a higher standard framework, designed originally for the payment companies, such as Visa and MasterCard, handling credit card information.

PCI DSS standard was created to prevent credit card fraud in industry organizations processes and card payments. It will increase controls around data and payment transaction exposure to compromise. The standard requirements concern all organizations that hold, process, or exchange cardholder information from any payment card brand. Organizations must have their compliance assessed by an independent assessor called by Qualified Security Assessor (QSA) or in the case of smaller company via a Self-Assessment Questionnaire (SAQ) (Almunawar and Tuan 2011).

PCI DSS is very specific to the payment card sector and it's only relevant to the payment part of a business systems. Usually PCI DSS is implemented in association with some other security framework.

5.1.6 NIST SP 800-53

NIST, U.S. National Institute of Standards and Technology has established a wide collection of information security standards and best practices. NIST SP 800-53 is a mature and very comprehensive standard and good for large sized businesses and especially for companies and businesses with US connection.

Other U.S. government agencies frameworks have evolved from NIST SP 800-53 standard. Bu utilizing NIST SP 800-53, one can comply with the Federal Information Processing Standard's (FIPS) 200 requirements. NIST 800-53 covers all FIPS Risk Management Framework steps that address the security controls. NIST 800-53 is specific to U.S. government agencies, yet, the framework could be applied to any other industry and particularly by the companies looking to build an information security program. NIST 800-53 is used by U.S. federal organizations to meet ISMS requirements (SearchSecurity 2017).

The strength for NIST is that, it has very detailed instructions to implement a framework and an organization not wishing to spend time on customizing a framework for their specific industry needs or nature may still have an adequate level of implementation details complimenting to its goals (Agnosticator 2017).

The weakness of NIST 800-53 is that it has limited the scope to information security, compared e.g. to COBIT and ITIL that are more general in nature. Multiple publications must be used, processed and implemented in order to achieve full compliance. That can easily lead to coverage gaps.

5.1.7 Comparison Conclusions

Security frameworks are vital for Information Security Management implementation and in order to be successful, the decision about, which to use, should not be left to IT teams only. As defined in ISMS, the boards and senior management need to be fully involved and responsible for the decisions. None of the security frameworks is mutually exclusive, so one needs to tailor one or more to suit one´s specific needs.

Each information security standard is plays its own role and position in ISMS implementation project. Standards, such as ISO 27001 and BS 7799 mainly focuses on information security management system domain, while PCI DSS focus on

information security relating to business transactions and smart card. ITIL and COBIT focuses more on information security requirements within the Project management and IT Governance (Almunawar and Tuan, 2011).

Referring to the usability of standards in global scope Appendix 2,, indicating that ISO 27001 is a leading standard, especially on ISMS and to the above mentioned standard

comparison information, the recommendation is to use ISO 27001 and ISO 27002 for ISMS establishment. The fact is that Media X Corporation have main businesses in the European economic area and therefore should use the standard that is more easily implemented and well recognized by different stakeholders.

6 ISO 27000 Standard Family

ISO/IEC 27000 series standard family consists of all together over 50 different documents. The ISO/IEC 27000 standards provide best practice recommendations on information security management, risk management and security controls within the context of an overall *Information Security Management System* (ISMS).

Part of the ISO/IEC 27000 family standards cover some other areas out of the information security scope, such as 27032: Guideline for cybersecurity, 27033: Network security, 27034: Application security, 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence. Appendix 1. presents the whole set of ISO/IEC 27000 standards (Suomen Standardisoimisliitto, 2015).

ISO/IEC 27000 standards do not expect any particular Information Security Management System structure but they are recommendations for an organization to build up and design their ISMS to best fit for their own business purpose. The standard forms a logical framework and best practices for defining the appropriate ISMS for the organization. Figure 2. presents ISO 27000 family of standards.

ISO 27000 standards guide the ISMS implementation based on strategic information management and governance targets. Those initial targets are described as *Information Security Policy*, *Risk Management Policy* and *Security organization* definitions. *Information Security Architecture* will be defined for the assets described in the above-mentioned documents.

After the policy and organization related definitions needed security technologies, controls, security targets and related processes can be defined more detailed. All this will be adapted to the existing organization and infrastructure. The basic requirement for the functional ISMS is that there is a pre-defined information security evaluation

process, which will reveal possible gaps in the activity and set up new targets for the ISMS development and personnel training (Suomen Standardisoimisliitto, 2015).

From information security point of view the most important standards are:

- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27005 — Information security risk management

Even the main target for the Media X Corporation ISMS improvement project was not to be fully compliant with ISO 27000, the ISO/IEC 27001 and ISO/IEC 27002 were the main documents to be followed and the existing security controls and activities were evaluated against the standard requirements and recommendations.

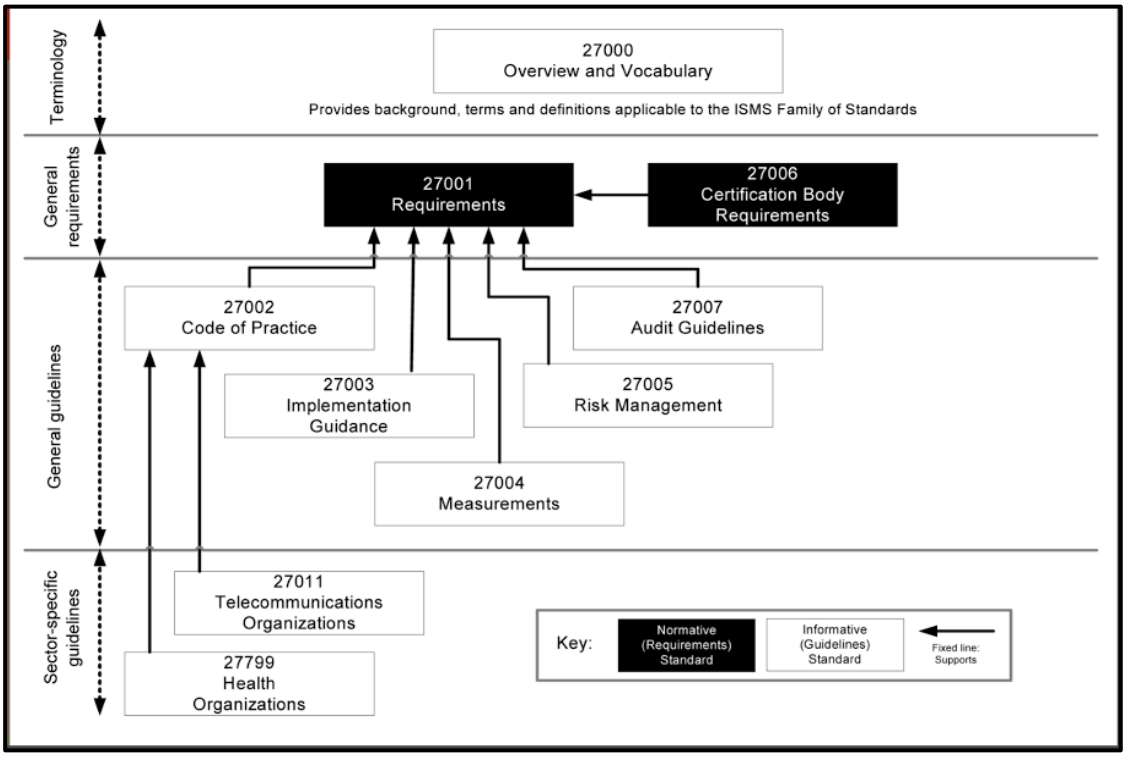


Figure 2. ISO 27000 family of standards categories (ISO 2015)

7 Standard Information Security Management System

ISO/IEC 27001 is an information security Management System standard published in September 2013 by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC). Its full name is ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 2015).

Operative Security Information Management System

The objective of ISO/IEC 27001:2013 standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISO/IEC 2015).

An Information Security Management System is a holistic approach to manage information security – *confidentiality*, *integrity*, and *availability* of information and data. ISMS is a part of the overall management system, based on a business risk approach. It is notable, that it does not focus on information technology alone, but also take into account other important business assets, resources, and processes within the organization. Figure 3. presents an operative Security Information Management System. A holistic overview of ISMS Implementation and Certification Process for ISO/IEC 27001 for implementing ISMS can be seen in Appendix 3.

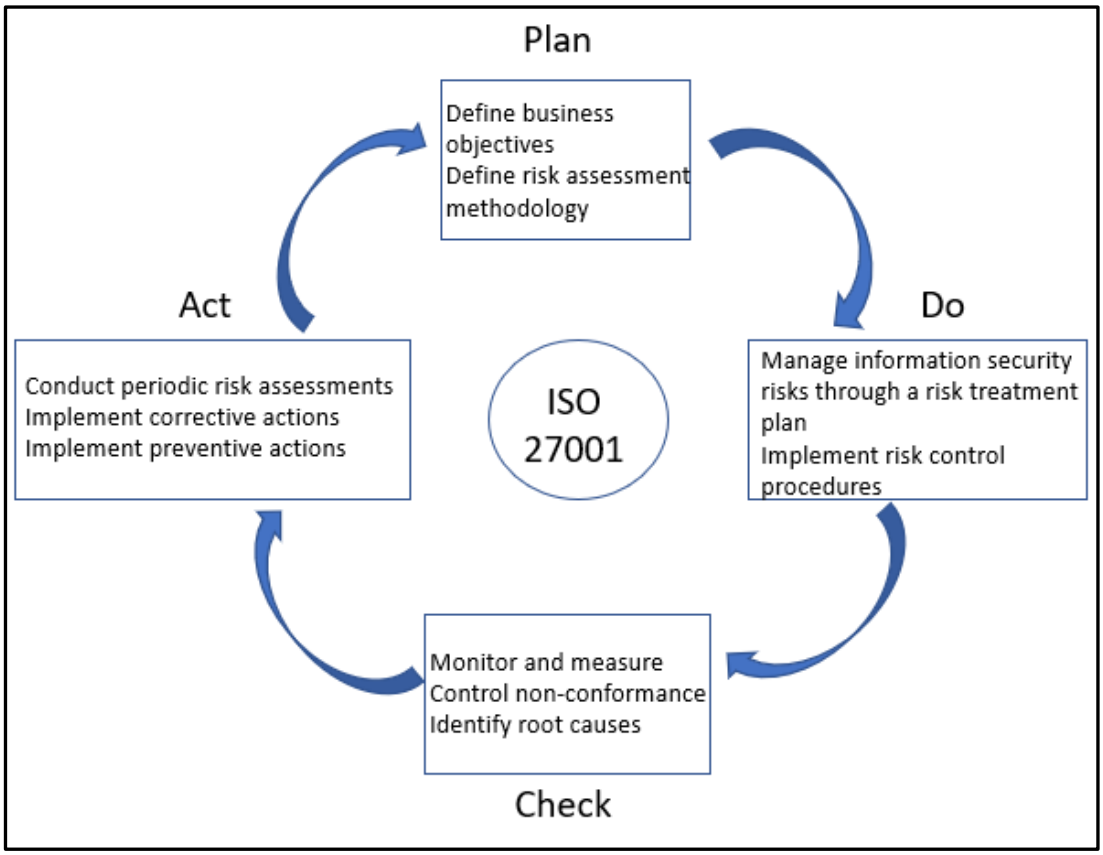


Figure 3. Operative Security Information Management System overview. (Google images, ISMS overview).

To successfully implement the ISMS, the organization has to go through several steps. Firstly, it needs to define and implement a risk assessment approach to identify and evaluate all threats and risks. Secondly, it needs to select appropriate controls and control objectives to mitigate the risks. Annex A of ISO/IEC 27001 defines all the controls that needs to be taken into a consideration when defining the Statement Of Applicability (SOA). SOA is a complete list of information security controls that are necessary for a company. In some cases, all of them they may not be applicable to an organization. The Last phase is to implement a P-D-C-A cycle (see Figure 3) and to continually improve information security (TUV Rheinland 2017).

Risk Management as a Basis of ISMS

The risk management consist of four processes. These processes are *risk analysis*, risk *assessment*, *risk reduction* and *risk evaluation*. Figure 4. is presenting the Risk Management process.

With a Risk Management Process, an organization can balance their operational and financial cost of security measures; in addition, their business mission goal can be achieved more safely and predictably. When risk management is not only bound by information technology and security rules, it helps enterprises to meet their goals and protect organization´s assets.

Risk Management also helps to identify, control and reduce the impact of different vulnerabilities. The main goal of this process is to minimize the risk by performing essential security activities or functions that can be approved and sponsored by the senior management. This way the control effort costs can be compared to the possible business impact costs caused by some particular risk caused by identified vulnerability (ISO27k forum 2017).

To fully implement ISMS, it is expected that a company has been evaluated its business risks including the information security risks, and the controls have been decided and developed accordingly to mitigate the risks in adequate and acceptable level. Hence, the starting point to run ISMS in a company is to evaluate the existing risks and to continuously improve and develop the security controls until the acceptable risk level is exceeded.

Many times, company ITs have implemented security controls, without any proper connection to company Business Risk analysis to mitigate the risks purely from IT functionality perspective only. This is not a completely wrong approach and in some scale of companies it can work out; however, in big companies and concerns the situation is different. In those cases, a part of the business-critical assets´ outside the IT scope, could be left out accidentally, or a part of the assets business criticality could never had been identified in practice. When assessing risks, all the essential assets for business should be inventoried and taken into a consideration in the overall risk picture.

The above-mentioned scenario was also the case with Media X Corporation before the Current State Analysis was started. Current State Analysis results were supposed to be the start up situation to further develop Media X Corporation´s ISMS as a method for continuous improvement of information security. As a generic recommendation, the information security risk visibility should be improved by implementing Information Security Risk Management process and including the information security risks as a part of generic Business Risk Management process. Figure 4 below is describing a generic Security Risk Management Process.

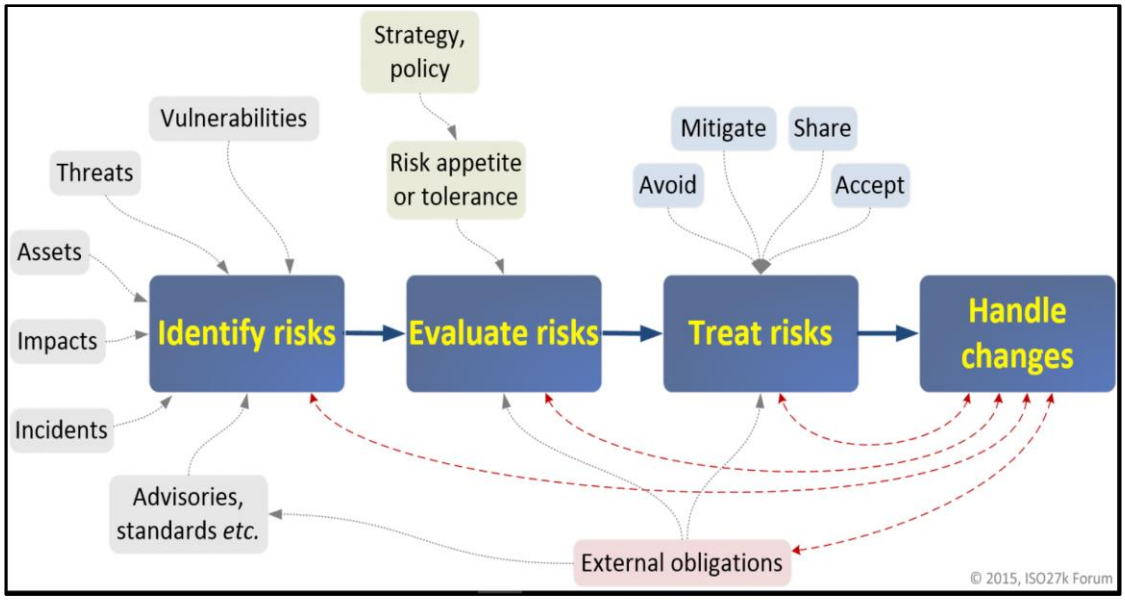


Figure 4. Security risk management process diagram. (ISO27k forum 2017)

8 Target for Media X ISMS Improvement Project

Security Policy standard statement: The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of the International Standard.

Main Focus of Improvement Project

The above-mentioned statement was recommended to be clearly stated in next version of Media X Corporation-wide *Information Security Policy* document that in turn

should be accepted as a part of formal commitment by Media X Corporation top management.

ISO 27001 standard and ISO 27002 code of practice specify the requirements for establishing, implementing, maintaining, monitoring, reviewing and continually improving the ISMS within the context of the organization, including assessment and treatment of information security risks.

The Current State report work was mandated by Chief Information Security Officer (CISO) of Media X Corporation and its main focus was on:

1. *Current State Analysis of the existing Information Security arrangement*
2. *According to the analysis work results to suggest some improvement for the existing Information Security arrangement*
3. *To guide the organization towards the ISMS ISO 27001 standard alignment*

To reach the ISMS target state, Media X Corporation organization needed to undertake the following steps in establishing, monitoring, maintaining and improving its ISMS:

- Identify and inventory all business-critical assets
- Identify information assets and their associated information security requirements
- Assess information security risks and treat information security risks to an acceptable level
- Select and implement relevant controls to manage unacceptable risks or to reduce risks to acceptable levels in some other ways, such as outsourcing some of the laborious controls to 3rd parties with agreements
- Monitor, maintain and improve the effectiveness of controls associated with the organization's information assets

Benefits of ISMS for Media X Corporation

The generic benefits (IT Governance 2017) for the Media X Corporation and any company that decide to deploy ISO 27001:2013 standard based Information Security Management System are:

- ISO 27001:2013 is one of the best frameworks for complying with legal, regulatory and contractual requirements of information security

- Laws and regulations continue to evolve to address information security and privacy risks
- ISO/IEC 27001:2013 is one of the best frameworks for complying with information security related legislation
- Better organizational image and possibility to get the official certificate issued by a certification body if decided to proceed until the official audit
- Proves that senior management are committed to the information security of the organization, including customer's data and information management
- More focus is placed reducing the risks for information that is confidential or otherwise valuable for the organization
- Provides a common security development goal for the Media X Corporation organization
- Operations are optimized within the organization because of clearly defined responsibilities and business processes
- A culture of information security for Media X Corporation is build
- In the long run it will be beneficial for corporate external image by keeping out the possible negative reputation and bad media visibility
- Help Media X Corporation to meet EU GDPR requirements

ISMS Current State Analysis and Evaluation Methods

The assessment was carried out in several interview sessions with the key persons. Auditor prepared questionnaires for the interviewing sessions. The questions apply to ISO 27002 best practices "Security Health Check".

The main questions to be answered were:

- What is the operative security awareness of the organization?
- What are the existing security controls in use?
- Are the existing security controls mitigating the risks enough?
- How are the existing security risks identified?
- How is information security managed within different parts of organization?

- Who owns the security assets in different parts of organization?
- What is the level of security co-operation within different parts of organization?
- How is the related security documentation managed?

To get an answer to above mentioned questions, the ISO 27002 requirements were compared to the collected interview results. The risk management related questions were out-scoped because Media X Corporation has not conducted an information security risk analysis in a systematic way, even though few areas have been identified and also evaluated as information security risks. Hence, no risk identification was done for the assets; neither were the risk mitigation controls relevant to evaluate.

In addition, there were some additional, more privacy related interview questions utilizing PCI DSS requirements. The questions were explained by the auditor, and the answers were recorded along with comments that were brought up during the discussions. Based on the result of the recorded interview the information security maturity levels and maturity values were defined for the chosen ISO 27002 control areas.

The studying methodology is based on an analysis of existing ISMS documentation, functions, roles, procedures and processes against the existing security policy, ISO/IEC27001 and ISO/IEC 27002 standards requirements.

The aim was not to follow the standard requirements slavishly but to adapt and recommend development areas for those parts fitting for the Media X Corporation business model best. The following generic documentation and tools were used as a guidance for the study of existing ISMS evaluation.

- ISO 27000 ISMS auditing guideline (ISO 27k 2017)
- ISO 27001 ISMS gap analysis tool (defined Excel tool to fit for the purpose of this assessment)
- ISO/IEC 27001:2013 standard (ISO/IEC 2015)
- ISO/IEC 27002:2013 code of best practices (ISO/IEC 2015)

The initial preparation work was information gathering by interviewing key personnel of Media X Corporation at different levels of the existing security governance and operative organization.

In addition, essential part of the study was defining of the existing security business domains of Media X Corporation, locate their key persons and assets as well as operative security controls, processes and procedures used within those different security domains and creating a holistic situation view for Information Security Management to help developing the most critical areas.

9 Media X ISMS Improvement Project

The ISMS improvement project Current State Analysis at Media X Corporation was divided into the following main phases:

Phase 1. Personnel interviews => Visibility to operative information security situation.

Phase 2. Documentation review => Visibility to existing controls, processes and procedures.

Phase 3. IT architecture and design => Visibility on domains and assets versus controls. Clarify owners of the control arrangements, IT Service descriptions, third party agreements, etc.

Phase 4. Collected information evaluation against ISO 27002 requirements, compare to existing Media X Corporation assets and controls and transfer the results to Current State evaluation tool.

Phase 5. Compile reported information results and wrap up the Current Sate report.

Phase 6. Presentation of the results of the Current State analysis for the assignee, CISO and his security team and the ISMS Current State Report for CISO.

Start Up Phase

Planning the scope of the Current State Analysis and identification of key persons to be interviewed were the very first tasks of the project. Also, all other project related

practicalities, such as physical access to Media X site premises in Helsinki, access credentials to Media X internal network, email accounts, availability of Media X work station and cost compensation during the project were agreed and arranged.

In addition, storage place for the needed information and documentation was established in Media X SharePoint environment. The project plan was prepared in cooperation with Media X Security Personnel and a tentative schedule for the project was accepted in October 2016. The more detailed project plan as well as the project execution schedule and follow up meeting practices were clarified and agreed more in detail during November 2016 so that the planned practical project activities could be started in the end of December 2016. (See Appendix 6. Removed for confidentiality reasons).

Interviews

The candidate key persons for the interviews were carefully selected from Media X Corporation´s IT security team as well as other departments in Finland relevant for the security study. The interview schedule and project plan were accepted with Media X Corporation CISO and with the interviewed Media X key persons.

Part of the interviews related to the current state analysis were held during the end of year 2016; most of them were scheduled for the beginning of year 2017. The interviews with the key persons started with the Media X Corporation´s security team members, who were already aware of the ISMS improvement project. The interviews with other area key persons continued during year 2017.

One of the most essential issues for a successful internal improvement project is the awareness and information sharing with the target organization about the planned activities. This is something that cannot be overestimated. Hence, the very first task was to inform the target organization personnel about the forthcoming interview activities well before the actual activities started.

Another important issue for this project was the upper management mandate for the planned project. Both these two issues were taken into consideration in Media X Corporation´s ISMS improvement project. Media X Corporation CISO had the confirmed mandate for the project from the top management and an introduction and

mandate letter was sent to Media X personnel who were to be interviewed. Appendix 5 (Removed for confidentiality reasons) presents the introduction and commitment letter. Table 2 (Removed for confidentiality reasons) introduces the list of interviewed key persons at Media X Corporation.

Media X Corporation Documentation Review

In the documentation review phase, all available information security and related IT documentation was gathered in to one security documents repository for documentation review purpose. There was no standard documentation structure implemented in Media X Corporation and one sub-task was to categorize the existing material to standard documentation categories. Figure 6 present the proposed new security and IT documentation structure.

The documentation was one essential criterion when evaluating the control area maturity. The lack of policy documentation, process documentation or operating procedures diminished the maturity points by one point. Because some of the control areas were under development, this was taken into consideration when evaluating the maturity impact on the control area documentation for the whole control area maturity as explained in Table 3.

As an example, if the control area evaluation result after the interview and self-assessment of the control area person is 7 and the area is still missing process (-1) and process documentation (-1) will decrease the final evaluation maturity value to level 5. Respectively, if the control area result of the responsible sub-contractor is 8 and the security requirements with agreement is missing (-1) as well the process description missing, (-1) the final evaluation maturity value is 6. The criteria and values of the information security maturity impairment are explained in Table 3.

Table 3. Documentation specific evaluation and maturity impairment criteria

Documentation:		Maturity impairment criteria	
Exits	Content or topic exists in policy or standard exist	Item missing from agreement or plan	-1
Draft exists	Standard, guideline exist as draft or topic will be updated	Process missing	-1
Planned	Standard, guideline or topic doesn't exist but it will be needed	Documentation missing	-1
Doesn't exist	Standard, guideline or topic doesn't exist	Control Plan missing	-1

Table 3 describe the criteria for the documentation evaluation used in this study and also the effect of a missing item for the maturity value of final information security in a specific area. The missing items diminish the final maturity value by one.

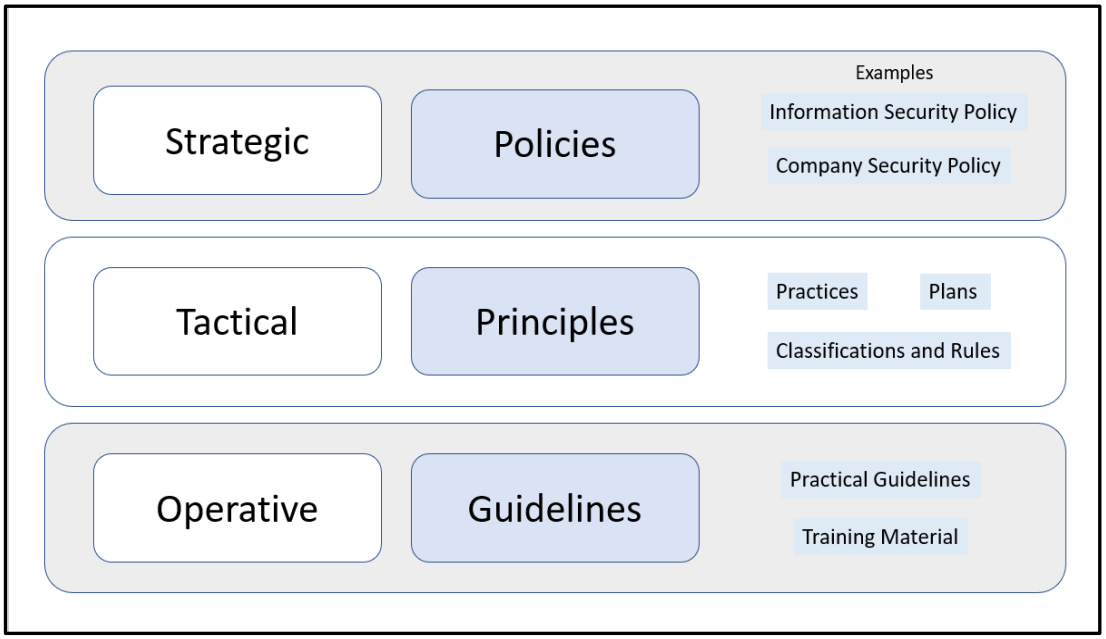


Figure 6. Proposed Media X Corporation documentation structure

In the document review all documented material was browsed through and document content and document availability were studied. Finally, all reviewed documentation was arranged to Media X Corporation´s SharePoint repository according to the categorization presented in Figure 6. This will be the security documentation structure of Media X Corporation.

Current State Results and Wrap Up

As a final phase of the project, the current state results were wrapped up and presented in a more detailed way for the Media X Corporation´s CISO and Security team in a project close-out meeting. There was also a possibility to comment the relevance and correctness of the findings. Some control case aspects were discussed; however, nothing was changed in the actual report. Appendix 8 presents part of the wrap up presentation (Removed for confidentiality reasons) and Appendix 9 presents

the cover sheet and content of the Current State report (Removed for confidentiality reasons).

10 ISMS Evaluation Tool

How to qualify and quantify the interview results to become more understandable? That is the question.

The basic comparison against plain ISO 27001 standard requirements or completeness level of the requirements of the ISO 27002 code of best practices gives a certain level of maturity results compared to a complete standard model. It does not state in which shape the organization is at the moment and it does not take into consideration the target company´s business specific nuances.

Evaluation of the Security Current State

The current state analysis should serve the information security management´s approach in the existing situation to establish an improved ISMS for Media X Corporation in the best way to fit for their purpose. This was the starting point when planning the evaluation criteria for the Current State tool evaluation. There are many commercial and non-commercial tools that could be used to help evaluate the security current state, however, here the main emphasize was put to give practical and most comprehensible results for the perspective of Media X Corporation security team to continue their approach to improve the existing information security situation. Appendix 7 (Removed for confidentiality reasons) presents an overview of the Current State Evaluation tool.

The Current State Evaluation tool is an Excel spreadsheet with definitions of ISO 27002 control area. There are altogether 12 separate interleaves for different control area questions. Each control area is valued according to the interview results and existing control area related documentation as well as possibly related process maturity situation. The sub-categories of each control area have been evaluated and the maturity value has been defined for them separately. Control area specific maturity

values are mean values of the all sub-category values specified for the respective main control area.

This operation increases the abstraction level so that it is easier to get an overall understanding of the control area situation as a whole instead of a bunch of more detailed sub-controls situations. Hence, the evaluation results become more descriptive and easier to present as a wrap-up for upper management, which is actually one of the target of the Current State report.

Evaluation Tool and Current Status Color Coding

In the Current State report, the following colour coding is in use to indicate the maturity level of the information security area based on ISO 27002 definitions. The actual service and function specific risk levels for the different business areas must be assessed separately before starting on a continuous improvement of ISMS.

Maturity Level Color Codes and Maturity Values

The maturity level colour code and respective maturity value criteria used to evaluate the maturity of the information security area is explained in Table 5. Security control status levels are categorised according to the cumulative points as follows: *Critical 0 - 2, Weak 3 - 5, Moderate 6 – 8, Good 9 – 10*. For these, please see Table 5.

It is notable that the expressed maturity levels of the ISMS areas in here do not necessary reflect the criticality level of business in that particular area, however, the business criticality shall be evaluated by a separate risk evaluation project as a part of further development work on ISMS. Some of the ISO 27002 control areas are not presented in the following table because of the limitation reasons of the project scope. In addition, the chosen main control categories are combination of suitable ISO 27002 control areas to be utilized better for Media X Corporation purpose.

Table 5. The colour code and respective evaluation criteria

Control Status generic:		
Critical		Control doesn't exist
Weak		Control area in weak security condition. Maybe planned, but not implemented, documentation and formal process missing
Moderate		Control area in moderate condition. Implementation ongoing, documentation or formal process missing
Good		Control implemented and communicated. Documentation and process exists. (Is it adequate? => Control shall be assessed)
Control Status details unwrapped:		
Critical		
0		**Control doesn't exist, Documentation or topic doesn't exist, formal process missing**
1		Control doesn't exist, but is on roadmap , formal process missing, Standard, guideline or topic doesn't exist,
2		Control doesn't exist, but under planning , formal process, Standard, guideline or topic doesn't exist
Weak		
3		**Control planned on roadmap, but not implemented, documentation and formal process missing**
4		Control area planned, but not implemented, Standard, guideline, topic defined on roadmap, formal process missing
5		Control area planned, but not implemented, Standard, guideline exist as draft or topic will be updated, formal process still missing
Moderate		
6		**Control implementation ongoing, documentation or formal process missing**
7		Control area implementation ongoing, formal process defined, Standard, guideline or topic doesn't exist but is on roadmap
8		Control area implementation ongoing, formal process defined, Standard, guideline exist as draft or topic will be updated
Good		
9		**Control implemented and communicated. Process does exist, Standard, guideline exist as draft or topic update on roadmap**
10		Control implemented and communicated. Documentation and process exists. (Is it adequate? => Control shall be assessed)

Table 5 defines the basic maturity of the evaluated area, and the numbering within the maturity area describes the justification of the criteria in more detail. This more detailed numbering shall provide the reader with better understanding, of where the possible gap or weakness is in comparison to ISO 27002 requirements.

It is also notable that even though the main information security control areas are on certain level as indicated in Table 5 there might be separate controls the maturity values of which differ radically. That is because the maturity value of each main control area consists of an average value of all area controls defined within the specific control area according to the ISO 27002 control listing. In the next chapter the maturity values of the ISO 27002 control areas are described more in detail.

11 Analysis Results of Information Security Current State

The Media X Corporation´s Current State analysis results are presented in the following tables (Removed for confidentiality reasons). The tables include earlier mentioned maturity color codes and maturity values of the sub-control areas. The main control area maturity values are presented in Table 14. (Removed for confidentiality reasons). The overall Media X Corporation´s information security situation is described in Figure 7. All following security control area tables are parts of the original Current State report of Media X Corporation.

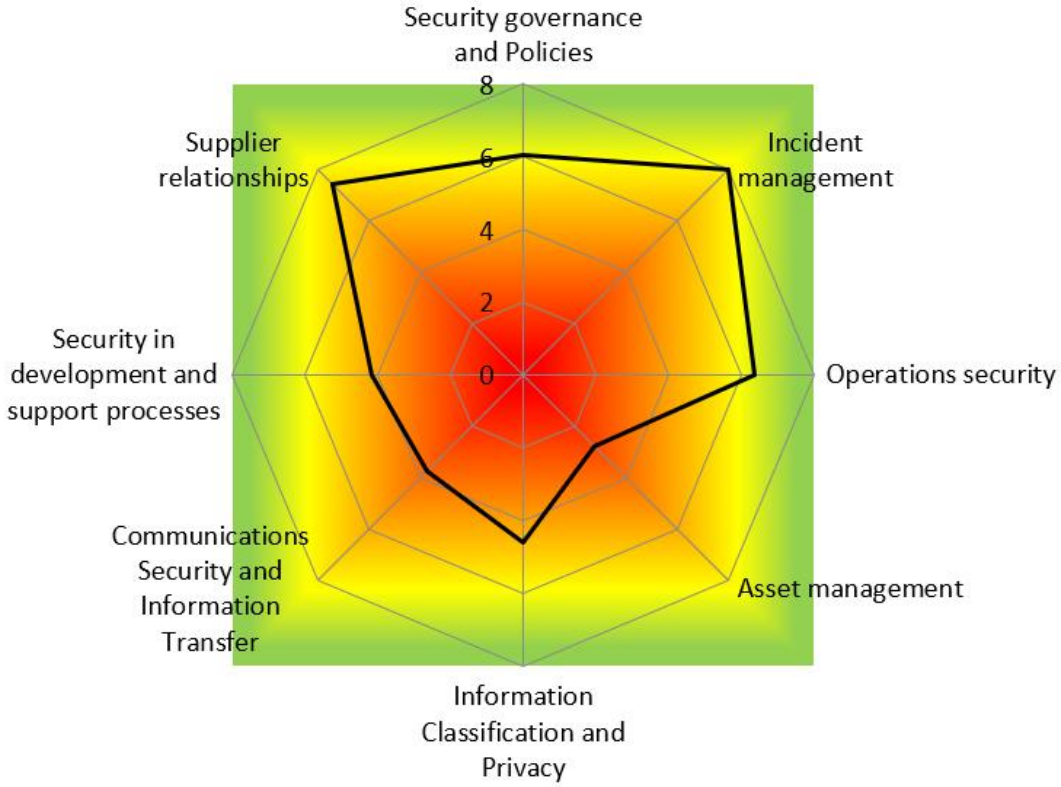


Figure 7. Overall situation of the Media X Corporation information security.

Table 14 (Removed for confidentiality reasons) and Figure 7 provide the generic overview of the current state of Media X Corporation´s information security. Some control areas, such as Incident management and Supplier relationships were generally in good shape, whereas control areas, such as Asset management, Communications

security and Information transfer as well as Security in development and support processes are need of improvement. The more detailed analysis and justification for the maturity values are explained in Media X ISMS Current State report (Henttinen 2017), which is not included here due to Media X *Company Confidential* document status.

12 Conclusions and Recommendations

There are several security frameworks available, such as COBIT, ITIL, PCIDSS, NIST, etc. Some of them have a wider focus on information security whereas others have a narrower scope and some of them have specialized in some specific business areas only. For the Media X Corporation´s business perspective the ISO 27001 turned out to be most useful and best suitable for the required purpose.

When starting an improvement project on information security, it is essential to find out the current state of the existing security controls. The generic *Current State Analysis* based on ISO 27001 standard is a good tool to be used for the purpose, however, it does not give all necessary answers automatically. It provides a good framework and checklist to accomplish all crucial tasks to be successful.

In addition, the understanding of the target company´s business environment, organizational structure and personnel inter-relationships as well as existing work pressure they are undergoing at the moment when the *Current State Analysis* is carried out is essential.

The project answered to the earlier mentioned main questions and targets successfully. The security awareness level of the target organization was defined. As a result, there was need for additional information security training and awareness creation.

Even the risk related evaluation was out-scoped as such. One of the findings was that the risk analysis of the core-components has been performed in a limited manner, and they were not accomplished regular basis, because the generic companywide process was missing. The existing security controls were recorded and the security

management organization structure was identified. In addition, different assets owners were identified and the co-operation level between the asset owning organizations and security organization was evaluated. The results revealed that there is room for improvement in the interrelationship and co-operation of different parts of Media X Corporation´s organization and also in asset management controls and tools. The special asset management project started to improve the situation. Finally, the existing Media X Corporation´s information security related documentation was inventoried, collected together and structured in a new recommended way.

The used ISMS current state evaluation tool was based on ISO 27002 control definitions. For this kind of current state study, it gave an adequate level of visibility and understanding about the existing situation, to be used as a basis for first ISMS improvement round.

From the project management point of view, the Current State Analysis project was successful. All project phases were accomplished according the planned schedule. The interviewed key persons were reached, and co-operation as well as the security attitude of each individual person was good. During the interviews the use of a recorder is recommended, especially when there is only one interviewer doing the notes as well as interviewing. In addition, it is crucial to get a deep understanding of the business organization mode of operations as well as the interrelationships of the different information security related teams to understand successfully the internal and external risks for the company. According to the CISO and Security team's positive comments the project reached the target and fulfill their needs in that phase of the ISMS improvement project. The Current State Analysis report (25 pages) itself was declared *company confidential* by Media X Corporation.

Media X Corporation has an information security organization, and the related responsible roles are defined as well as operative security work partly outsourced and responsibilities to cover the most important functions and to meet at least the minimum information security requirements to run the business. In the operation area, there are standard IT security controls partly in place. This applies also to the externally hosted areas and cloud environments as well as controls implemented within in house IT domains.

The importance of information security is understood, and activities to improve the existing situation have been started; yet, the implementation in many areas is still uncompleted, which also applies to respective process and documentation situation.

Although, the daily operative information security tasks can be accomplished in practice, there are no additional or extra contingency activity related resources available in the organization, e.g. in case of temporary unavailability situations of personnel. As an implication, certain persons have several operative information security roles, and their responsibilities cover different control area responsibilities in practice. *This is a critical, generic operative level finding.*

According to the knowledge and experience collected from several other alike projects. The described situation about the situation with generic security resources is too common in other companies also.

Another generic level finding, according to the interviews, is that overall security awareness within the personnel outside of the Media X Media internal information security "community" is not at an adequate level at the moment. In practice, this appears as reluctance to recognize information security caps as business risks. As a finding, *the Media X Corporation Business Risk Management process has no connection to information security risks and in that sense information security risks are not well understood and recognized outside the information security "community".*

What comes to *Security Awareness* improvement, one cannot underestimate the importance of the basic level security competence and knowledge in the context of overall information security adaptation as a part of normal business processes and practices. It will improve personnel´s attitude against the information security as well as top-level management´s awareness of information security risks and commitment to maintain security issues, when planning new e-business opportunities for the corporate business strategy.

The Current State report results reflect very well the original project objectives mentioned in section 3 - *Objectives of the study*. The report is an overview of Media X Corporation´s Information Security situation. The different gaps in security control area were presented and the improvement proposals were done respectively. The report also throws some light on the control areas lacking adequate management

visibility, and the current state project itself improves the security team´s awareness and as well as other team's awareness of the existing security situation, which was also one of the project objectives.

Introduction of new web-based service technologies and concepts to company service portfolio is opening up new doors for business opportunities and enriching the company´s brand and image; however, in the same time, if the information security risks are not taken into account and if necessary security controls are neglected a Pandora's box of failure can open. It might be impossible to compensate bad image within the consumers and customers, which can lead business come-downs in the worst case, not to mention possible sanctions and fines placed by authorities in case of serious data breaches. Hence, it is worth to taking the EU GDPR requirements seriously when planning security controls for the company business assets.

Following ISO 27001 standard recommendations, when defining company security controls, it is providing a tool set for basic information security improvement. Even the main approach would not target an audit compliance of full ISO 27001 standard, it can still bring about the basic GDPR compliance and improve the visibility and understanding of the security and privacy related aspects of the company.

References

Agnosticator, 2013. A Comparison of COBIT, ITIL, ISO 27002 and NIST, Agnosticationater.blogspot.fi. Accessed on 9.11.2017. Retrieved from http://agnosticationater.blogspot.fi/2013/12/a-comparison-of-cobit-itil-iso-27002.html

Almunawar and Tuan, 2011. Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05. Accessed on 10.10.2017. Retrieved from https://s3.amazonaws.com/academia.edu.documents/30294093/113505-6969-ijecs-ijens.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1516299442&Signature=Uk0s3FOpJKly2%2FOrlBXO%2FK1MJWM%3D&response-content-disposition=inline%3B%20filename%3DInformation_security_management_systems.pdf

Clarke, 2005. Research Models and Methodologies, HDR Seminar Series: Faculty of Commerce. Retrieved from http://www.uow.edu.au/content/groups/public/@web/@commerce/documents/doc/uow012042.pdf

Faculty of Commerce, 2012. Qualitative VS Quantitative, Research Methodologies, their differences and uses, HDR Seminar Series. Retrieved from https://www.slideshare.net/eilire91/qualitative-vs-quantitative

Government of South Australia, 2017. Information Security Management Framework. Retrieved from https://digital.sa.gov.au/sites/default/files/content_files/policy/ISMF-v3.3.pdf

Google search, Information security. Accessed 15.9. 2016. Retrieved from https://en.wikipedia.org/wiki/Information_security

Google search 2. Information security risk assessment guidelines. Accessed 20.3.2017. Retrieved from http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html

Henttinen H., 2017. Media X ISMS Current State report (Media X Confidential).

Henttinen H., 2017. Media X Current State Analysis Wrap up presentation, (Media X Confidential).

Henttinen H., 2017. Current State Analysis Tool, (Media X Confidential).

HiTrust, 2017. Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/CSFComparisonWhitpaper.pdf

ISO 27k, 2017. ISMS Auditing Guideline version 2. Retrieved from www.iso27001security.com/ISO27k_Guideline_on_ISMS_audit_v2.docx

ISO/IEC 2015. ISO/IEC 27001 —2013 Information technology - Security Techniques - Information security management systems — Requirements. Retrieved from https://www.iso.org/standard/54534.html

ISO/IEC 2015. ISO/IEC 27002 —2013 Code of practice for information security management. Retrieved from https://www.iso.org/standard/54533.html

IT Governance, 2017. The benefits of implementing an information security management system (ISMS). Accessed 23.9.2018. Retrieved from https://www.itgovernance.co.uk/isms-benefits

Media X Corporation, 2017. Media X Corporate Governance Statement. Accessed 14.11.2017. Retrieved from https://www.Media X.com/en/investors/corporate-governance

Media X Corporation, 2017. Who we are. Accessed 14.11.2017. Retrieved from https://www.Media X.com/en/who-we-are/areas-expertise

NIST, 2017. Framework for Improving Critical Infrastructure Cybersecurity, 3-5. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST, 2017. NIST Cybersecurity Framework, 3-5. Retrieved from https://www.nist.gov/cybersecurity-framework

NIST, 2017. NIST Cybersecurity Framework/Cybersecurity Framework Excel. Retrieved from https://www.nist.gov/document-3764

NIST,2017. Cybersecurity Framework FAQs Framework Components. Retrieved from https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components

Origin, 2017. Six Most Common Security Frameworks Explained. Accessed 4.12.2017. Retrieved from https://originit.co.nz/the-strongroom/six-most-common-security-frameworks-explained/

Secuilibrium, 2017. Comparing NIST's Cybersecurity Framework with ISO/IEC 27001. Accessed 1.12.2017. Retrieved from http://www.secuilibrium.com/news/comparing-isoiec-27001-with-nists-cybersecurity-framework

SearchSecurity, 2017. IT security frameworks and standards: Choosing the right one. Accessed 5.12.2017. Retrieved from http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Suomen Standardisoimisliitto, 2015. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 – standardiperhe, Kalvosarja oppilaitoksille. Retrieved from http://www.sfsedu.fi/opetusaineistot/it-standardit

TUV Rheinland, 2017. Benefits gained from implementing an ISMS leaflet. Retrieved from https://www.tuv.com/media/india/informationcenter_1/systems/ISMS.pdf

Appendices

Appendix 1. ISO/IEC 27000 series standards (Suomen Standardisoimisliitto, 2015)

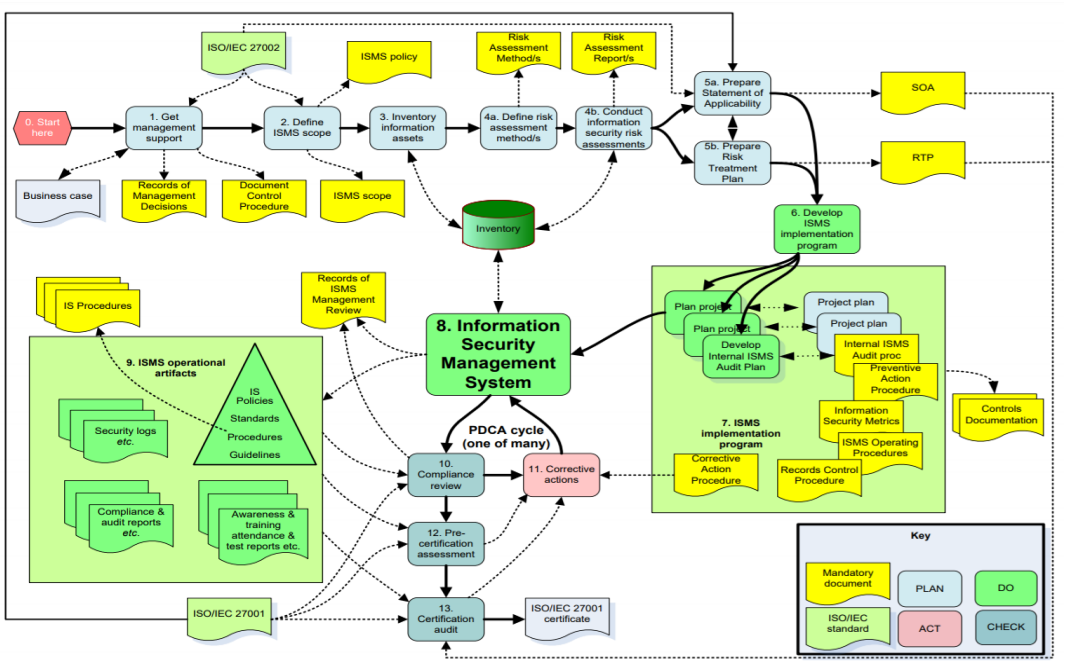
- ISO/IEC 27000— Information security management systems — Overview and vocabulary
- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements. The older ISO/IEC 27001:2005 standard relied on the Plan-Do-Check-Act cycle; the newer ISO/IEC 27001:2013 does not but has been updated in other ways to reflect changes in technologies and in how organizations manage information.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014 — Information security governance.
- ISO/IEC TR 27015 — Information security management guidelines for financial services
- ISO/IEC 27017 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032 — Guideline for cybersecurity
- ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts
- ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

- ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
- ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security
- ISO/IEC 27034-1:2011 Part 1: Overview and concepts
- ISO/IEC 27034-2:2015 Part 2: Organization normative framework
- ISO/IEC 27034-3 Part 3: Application security management process
- ISO/IEC 27034-4 Part 4: Application security validation
- ISO/IEC 27034-5 Part 5: Protocols and application security controls data structure
- ISO/IEC 27034-5-1 Part 5-1: Protocols and application security controls data structure -- XML schemas
- ISO/IEC 27034-6 Part 6: Security guidance for specific applications
- ISO/IEC 27034-7 Part 7: Application security assurance prediction
- ISO/IEC 27035 — Information security incident management
- ISO/IEC 27035-1 Part 1: Principles of incident management
- ISO/IEC 27035-2 Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 27035-3 Part 3: Guidelines for CSIRT operations
- ISO/IEC 27036-3 — Information security for supplier relationships
- ISO/IEC 27036-1:2014 Part 1: Overview and concepts
- ISO/IEC 27036-2:2014 Part 2: Requirements
- ISO/IEC 27036-3:2014 Part 3: Guidelines for information and communication
- ISO/IEC 27036-4:201427036-4 Part 4: Guidelines for security of Cloud services technology supply chain security
- ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27038:2014 - Specification for digital redaction
- ISO/IEC 27039:2015 - Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040:2015 - Storage security
- ISO/IEC 27041:2015 - Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27042:2015 - Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 - Incident investigation principles and processes
- ISO/IEC 27044 - Guidelines for Security Information and Event Management (SIEM)
- ISO/IEC 27050-1 - Electronic discovery - Part 1: Overview and concepts
- ISO 27799 — Information security management in health using ISO/IEC 27002. The purpose of ISO 27799 is to provide guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.

Appendix 2. Profile of big five of ISMS standards (Almunawar and Tuan, 2011)

	ISO 27001	BS 7799	PCIDSS	ITIL	COBIT
Profile of Standards	ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government; also other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations [8]	BS Standards is the UK's National Standards Body (NSB) and was the world's first. BS Standards works with manufacturing and service industries, businesses, governments and consumers to facilitate the production of British, European and international standards [13]	is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help industry organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise [20]	ITIL is the abbreviation for the guideline IT Infrastructure Library, developed by CCTA, now the OGC (Office of Governance Commerce) in Norwich (England) developed on behalf of the British government. The main focus of the development was on mutual best practices for all British government data centers to ensure comparable services [19]	is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT [9]
Initiated by	delegates from 25 countries [8]	United Kingdom Government's Department of Trade and Industry (DTI) [13]	**VisaCard, MasterCard, American Express, Discover Information** and Compliance, and the **JCB**Data Security Program [20]	The Central Computer and Telecommunications Agency (CCTA), now called the Office of Government Commerce (OGC)– UK [19]	Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)–USA [9],[14]
Launched on	February 23, 1947	1995	15 December 2004	1980s	1996
Standards & Components	**18,500 International Standards** [8],[15],[17]	**27,000 active standards** [13],[16]	**6 main components on standard** [20],[21]	**8 main components + 5 components version 3** [10],[18], [19]	**6 main components on standard** [10],[22],[23]
Certificate Name	Certificate of ISO 27000 Series	Certificate of BS 7799: 1-2	Certificate of PCI-DSS Compliance	Certificate of ITIL Compliance	Certified Information Systems Auditor™ **(CISA®)** Certified Information Security Manager® **(CISM®)** Certified in the Governance of Enterprise IT® **(CGEIT®**) Certified in Risk and Information Systems Control TM **(CRISCTM)**
Scope	Information Security	Information Security	Information and Data Transaction Security on debit, credit, prepaid, e-purse, ATM, and POS	Service Management	IT Governance
Usability	163 national members out of the 203 total countries in the world	110 national members out of the 203 total countries in the world	125 countries out of the 203 total countries in the world	50 international chapters	160 countries

Appendix 3. ISMS Implementation and Certification Process (Google search 2, 2017)



Appendix 4. Comparison of HITRUST, ISO & NIST Factor Definitions (HiTrust 2017)

1 Factor Definitions:

• ISO 27001-Based – Is the framework based on the international standard?

• Integrated Compliance Framework – Have multiple regulatory, standards, frameworks and best practices been incorporated into the framework?

• Healthcare Specific – Was the framework designed to accommodate the specific, unique needs of the healthcare industry?

• Healthcare Standard – Does the framework have significant adoption within the industry?

• Prescriptive – Are the framework control requirements sufficiently detailed to reduce ambiguity in implementation?

• Controlled Scaling – Can the framework be scaled to the specific needs of a healthcare organization in a centralized, pre–defined way?

• Controlled Tailoring – Does the framework allow the replacement of specified controls with alternate controls in a centralized, pre–defined way?

• Control Compliance-Based – Is risk determined through a gap–analysis of the control requirements and the maturity with which they're implemented?

• Organizational Certification – Does the framework provide for formal certification of the state of control compliance within an organization?

• Supports Third Party Assurance – Does the framework provide an adequate mechanism for the sharing of reasonably accurate and consistent risk

information amongst organizations?

• Assessment Guidance – Does the framework provide prescriptive guidance on how controls should be assessed through documentation reviews,

observation, interviews or testing?

• Tool Support – Availability of specific tools organizations may use to assess and manage controls and risks to the organization.

2 Additional guidance for healthcare is provided separately (ISO/IEC 27799 & NIST SP 800-66)

3 HITRUST is rapidly becoming the de facto standard for the healthcare industry

4 NIST and OCR collaborate on specific tools like the HSR Toolkit but do not promulgate NIST SP800-66 as an industry standard for healthcare

5 ISO 27001 provides relatively general requirements compared to NIST and HITRUST

6 Only HITRUST scales control requirements based on organizational, system and regulatory risk factors7 ISO compliance

7 Only HITRUST provides a formal, central review and approval process for alternative controls

8 ISO compliance is based primarily on an evaluation of the ISMS rather than on a gap analysis of the controls and subsequent risk to the organization

9 CSF Assessor organizations are not required to use the general guidance provided in ISO/IEC 27008